

New Iowa center keeps watch for hackers, Internet outages



Matthew Patane, mpatane@dmreg.com

7:53 p.m. CDT August 13, 2015



Nasty weather, unaware farmers and construction workers, hackers looking to steal information — there's no end of threats facing Iowa's state-run Internet network, which supplies an information lifeline to public safety agencies, schools and hospitals.

Knowing that outages and stolen information can ruin lives, the state's public Internet service, Iowa Communications Network, has set up a 24/7 watchdog center. Called the Broadband Information Center, it can instantly pinpoint breakdowns and hacks, and employees can quickly work to fix the problem.

(Photo: Rodney White/The Register)

The resulting real-time monitoring can keep the broadband network up and running even in the face of tornadoes, backhoes and cyberattacks, said ICN's executive director, Ric Lumbard, while giving The Des Moines Register an exclusive look at the system.

That's important in an age where hackers have stolen millions of pieces of personal information, victimizing major retailers, insurance companies and even the U.S. government, security and information experts say.

"It really matters, because if you let someone's attack run for an hour before you shut it down, they might break into 20 systems. ... If you can shut them down in 20 seconds, you might actually foil them, and they might not get anywhere," said Doug Jones, an associate professor of computer science at the University of Iowa.

'Truckload' of data travels across ICN

Sitting in an office building just east of the Iowa Capitol, the center can track outages, weather updates, bandwidth usage and cybersecurity attacks — all in real time.

"That requires us to have a highly visible environment. ... We have to be able to respond now and take action," Lumbard said.

[Buy Photo](#)



Ric Lumbard, Exec. Director of Iowa Communication Network, and the ICN's Broadband Information Center in the Grimes State Office Building, Des Moines, Iowa, Aug 7, 2015. (Photo: Rodney White/The Register)

The seven-person center is a new addition for the ICN, Iowa's dedicated telecommunications network for government agencies, schools and more.

Screens on the wall flash maps of Iowa, crisscrossed by lines that represent fiber cables carrying data to and from universities, hospitals and public safety officials. If a fiber connection is cut or disturbed, the line shines red, indicating a problem.

"This has a truckload of information," Lumbard said.

Center helps speed detection of problems

Lumbard said the agency started planning the center in 2013. It went online earlier this year.

"To me ... it's all about taking advantage of technology to get people collaborating more quickly and literally seeing the same thing," said David Marley, ICN's network operations manager.

For example, if the ICN can track an incoming tornado, officials can send someone to move equipment out of its path, stopping potential outages before they happen.

Quick responses are also critical in the case of a cyberattack or data breach.

With cyberattacks, "we don't have six hours. We have sites that are getting hit and they're down now and we have to respond in minutes. ... If you don't have fast notification, you can't track it, stop it, mitigate it. By the time you get the Band-Aid out, they're gone," Lumbard said.

[Buy Photo](#)



The Iowa Communications Network's Broadband Information Center in Des Moines includes large screens for monitoring. (Photo: Rodney White/The Register)

While a number of recent cyberattacks were aimed at the private sector — Target, Neiman Marcus, multiple health care companies — government entities are ideal targets.

"We collect millions of records for all citizens and businesses in Iowa. We have medical information, we have security numbers, we have driver's licenses, all these mandated things that establish who you are," said Jeff Franklin, Iowa's chief security information officer.

In one recent 24-hour period, Franklin said his office received 280,000 alerts of potentially malicious activity, ranging from poorly written computer applications to harmful programs such as malware and trojans.

Once his office sees those alerts, Franklin said it filters through them to see what alerts could reflect the most harm.

"It's a big deal. We're trying to protect that every day," he said.

Hackers gained access to the Iowa Racing & Gaming Commission's computer systems in 2010, compromising the personal information of 80,000 people.

In 2012, a breach hit South Carolina's Department of Revenue, affecting millions of Social Security numbers.

The federal government suffered a more recent, more drastic breach. The Office of Personal Management revealed a few months ago that a hack compromised more than 20 million records.

The ICN represents a special case. Even though the ICN may not have a wealth of data, it connects to those that do.

"They're the transport. They're the highways. That's why they're critical in this," Franklin said.

System is 'under attack 24/7/365'

The difficult nature of protecting information makes it a constant fight, cybersecurity experts have said.

Attackers have to be right only once to successfully break in; protectors have to be correct constantly to keep them out.

"The reality is we are under attack 24/7/365. ... It's important to understand that we're always on the defensive," Franklin said.

Lumbard called it "constant pressure."

"There are always people, systems, computers, malware looking for vulnerabilities," he said.

Security professionals are also dealing with a variety of attacks, from phishing emails to denial of service attacks to spear phishing attacks, which use personal information to go after a specific target.

All of those are geared toward affecting information in some way, Jones said.

"What's my goal: to shut it down, to corrupt it or to steal from it? Those are the basic goals you can have," Jones said.

It's a threat Lumbard said the ICN recognizes.

"Intrusion detection is really the name of the game," Lumbard said. "If you don't know what's going on, you're not going to mitigate it. If you don't know somebody's in your house, you're not going to do anything about it."

All about the ICN

What: The Iowa Communications Network is Iowa's state government broadband carrier network, providing high-speed broadband Internet, data, video conferencing and phone services to public schools, higher education, hospitals and clinics, state and federal government, National Guard armories and libraries.

Where: The network makes up an estimated 8,661 miles of fiber cable — 3,400 owned by the state of Iowa and 5,261 leased.

Growth: ICN's bandwidth sales and data services have more than doubled in the past two years, and the amount of Internet purchased by authorized users has increased 165 percent during that time.

Who: Seventy-nine percent of the Internet provided by ICN is used by educational entities.

Source: Iowa Communications Network

Read or Share this story: <http://dmreg.co/1TxIN0c>